"Remote Access Vulnerability" ช่องโหว่ระบบที่หลายคนมองข้าม

by A.Pinya Hom-anek, GCFW, CISSP, CISA

ACIS Professional Team

E-mail: prinya@acisonline.net

การเข้าใช้งานระบบคอมพิวเตอร์ผ่านทาง Remote Access เช่น การติดต่อเข้าระบบโดยการใช้ Modem จากเครื่อง PC/Notebook เข้าสู่ Remote Access Server ขององค์กร หรือติดต่อผ่านทาง Internet โดยใช้ VPN หรือ SSL Protocol ในการเข้ารหัสข้อมูล ตลอดจนการติดต่อผ่านทาง LAN ของอีกระบบหนึ่งซึ่งเชื่อมโยงกับระบบอินเทอร์เน็ตต่อมายังองค์กร รวมทั้งการติดต่อเข้าระบบผ่านทาง LAN ขององค์กรเองก็ล้วนหมายถึง การเข้าใช้งานคอมพิวเตอร์จากระยะไกลที่ไม่ได้ Log On ที่ตัวเครื่องนั่นเอง

การติดต่อกับระบบผ่านทาง Remote Access นั้น มีช่องโหว่หลายประการที่แฮกเกอร์สามารถฉวยโอกาสในการเจาะระบบของเราได้อย่างง่ายดาย วิธีการเจาะระบบ Remote Access โดยทั่วไป ได้แก่

1. การดักจับ Username และ Password ในช่วงเวลาการทำ Authentication แฮกเกอร์สามารถใช้โปรแกรมประเภท Password Sniffer ดักจับข้อมูลของเรา หากเราใช้ Authentication Protocol ที่ไม่มีการเข้ารหัส เช่น PAP (Password Authentication Protocol) เป็นต้น

2. การดักจับข้อมูลในจังหวะที่มีการส่งข้อมูลที่ไม่ได้เข้ารหัส (หลังจากผ่านขั้นตอน Authentication มาแล้ว) หากเราไม่ได้ใช้ VPN หรือ SSL Protocol แฮกเกอร์สามารถดักจับ ตรวจดูข้อมูลของเราได้ทั้งหมด เนื่องจากข้อมูลที่มีอยู่ในรูป Digital Format นั้น สามารถ Copy ได้อย่างง่ายดาย โดยที่เจ้าของข้อมูลนั้นไม่รู้ตัวเลยด้วยซ้ำ ในปัจจุบัน แฮกเกอร์สามารถดักจับข้อมูลที่เข้ารหัสด้วย SSL Protocol เช่น ใช้ HTTPS ก็สามารถโดนดักจับด้วยวิธี "Man-In-The-Middle Attack"

3. เปิด Modem ทิ้งไว้ในระบบ LAN เพื่อที่จะหมุนโทรศัพท์ติดต่อเข้ามาโดยไม่ต้องผ่าน Firewall วิธีนี้กำลังเป็นที่นิยมในหมู่แฮกเกอร์ เพราะตรวจสอบได้ยากว่าใครเปิด Modem และต่อสายโทรศัพท์ทิ้งไว้ในองค์กร นอกจากจะตรวจคอมพิวเตอร์ทุกเครื่องโดยการเดินไปตรวจทุกเครื่อง ซึ่งเป็นไปได้ยาก ในปัจจุบันเราสามารถใช้โปรแกรม Vulnerability Scanner บางตัวในการตรวจสอบว่ามีการเปิด Modem ทิ้งไว้หรือไม่ หรือทดสอบระบบโดยวิธีการ War Dialing

4. การกำหนดนโยบายความปลอดภัย หรือ Security Policy ที่อ่อนเกินไปหรือไม่เท่ากันในแต่ละบุคคลหรือแต่ละอุปกรณ์ Remote Access หมายความว่า เราอาจเผลอกำหนด Remote Access Policy ไม่เหมือนกันในอุปกรณ์ Remote Access แต่ละอุปกรณ์ซึ่งมีการติดตั้งต่างช่วงเวลากัน ตลอดจนการไม่ได้บังคับใช้ Authentication Protocol ที่มีความปลอดภัยในการทำ Authentication เป็นต้น

5. ระดับความปลอดภัยของระบบหลัง Firewall หรือบริเวณ DMZ ลดลงเท่ากับระดับความปลอดภัยของ Dial-In Remote Access Client ซึ่งเป็นอันตรายอย่างสูงกับระบบ LAN ภายในองค์กร หมายความว่า หาก Dial-In Client เกิดติดไวรัสขึ้น อาจเกิดจากการเล่นอินเทอร์เน็ตที่บ้านโดยไม่ระวัง เมื่อ Dial-In Client ติดต่อเข้าสู่ Remote Access Server ขององค์กร และได้รับหมายเลข IP Address ภายในองค์กรไปใช้ในการต่อเชื่อมกับระบบภายใน ไวรัสก็สามารถแพร่กระจายเข้าสู่ระบบได้อย่างง่ายดาย และ ถ้าไม่ใช่แค่เรื่องไวรัส แต่เป็นแฮกเกอร์ที่เป็นมนุษย์ก็ยิ่งอันตรายมากขึ้น เพราะแฮ็กเกอร์สามารถเจาะระบบผ่านทาง Remote Access ได้อย่างง่ายดาย ยกตัวอย่างเช่น แฮกเกอร์สามารถเข้ามาแก้ไข Routing Table เพื่อเปิดเส้นทางส่งข้อมูลจาก Remote Access ผ่านเข้าระบบภายในขององค์กร วิธีการนี้ในเชิงเทคนิคเรียกว่า "Split Tunneling"

6. มีระบบป้องกันที่ดี แต่กลับถูกถล่มด้วย DoS (Denial of Service) Attack หมายถึง การที่เรากำหนด Remote Access Policy ไว้อย่างเข้มงวดว่า User ต้องไม่ Login ผิดเกินกี่ครั้ง ยกตัวอย่างเช่น หาก User ใส่ Password ผิดเกิน 3 ครั้ง ระบบก็จะ "LOCK" User Account นั้นทันที (คล้ายๆ กับระบบบัตร ATM ที่เราใช้กันอยู่ทุกวันนี้) ปัญหาก็คือ ถ้าแฮกเกอร์แกล้งใส่ Password ผิดๆ มากกว่า 3 ครั้ง User Account ตัวจริงนั้นก็ใช้ไม่ได้ทันที เรียกว่า แฮกเกอร์ต้องการทำ DoS Attack กับระบบ แต่ไม่ได้ต้องการทราบ Password ของ User นั่นเอง

7. ถูกขโมย Laptop หรือ Notebook ซึ่งมีการเก็บรหัสผ่านไว้ หรือกำหนดเป็น Auto Login ไว้ แฮกเกอร์ก็สามารถใช้ User Account ของเจ้าของเครื่อง ในการติดต่อเข้าสู่ระบบได้อย่างง่ายดาย

8. Remote Access User ไม่ใช่ตัวจริง เวลาเชื่อมต่อกับระบบ หมายความว่า User บางคนชอบบอก Password กับพี่น้อง หรือ ญาติมิตรเพื่อให้สามารถติดต่อเข้าระบบ และเล่นอินเทอร์เน็ตได้ฟรี โดยไม่ต้องเสียเงินหมุนเข้า ISP ซึ่งทำให้เกิดปัญหา Remote Access Server ไม่พอใช้ หรือเกิดปัญหาติดไวรัสในระบบเนื่องจาก User ไม่มีความระมัดระวังเพียงพอ

คราวนี้เรามาดูวิธีการแก้ปัญหา และการวางนโยบายรักษาความปลอดภัยในการใช้งานระบบ Remote Access กันบ้าง

1. ใช้ RADIUS Protocol หรือ TACACS+ Protocol ในการทำ Authentication, Authorization และ Accounting เพื่อตรวจสอบ Remote Access User, กำหนดสิทธิในการใช้งาน และเก็บประวัติการใช้งาน เพื่อการ Audit ต่อไป แต่ต้องระวังการดักจับ RADIUS Traffics ระหว่าง RADIUS Server และ Remote Access Server ด้วย

2. กำหนดกฎเหล็ก "Remote Access Policy" หมายถึง กำหนดตั้งแต่เบอร์โทรศัพท์ (Caller-ID) ที่สามารถติดต่อกับ Remote Access Server ได้, กำหนดระยะเวลาในการให้บริการ Remote Access, กำหนด Authentication Protocol ที่มีความปลอดภัยจากการ Replay Attack ของพวกแฮกเกอร์ ตลอดจนกำหนดสิทธิในการเข้าถึงส่วนต่างๆ ของระบบภายในองค์กร โดยผ่านทาง Remote Access และหมั่นตรวจสอบ Log เพื่อตรวจดูการใช้งานว่ามี User แปลกๆ เข้ามาใช้งาน หรือไม่ก็ตรวจสอบความผิดปกติ เช่น มีการใช้งานในช่วงเวลาที่ไม่ปกติจากการใช้งานโดยทั่วไป เป็นต้น

3. เข้ารหัสข้อมูล โดยใช้ L2TP และ IPsec Protocol หรืออย่างน้อยให้ใช้ SSL Protocol ในการส่งข้อมูล เพื่อป้องกันไม่ให้แฮกเกอร์สามารถดักจับข้อมูล Plain Text ได้ 4. ใช้ CA (Certificate Authority) ในการออกใบรับรอง Digital Certificate ให้กับ Remote Access Client และ Remote Access Server หรือ RADIUS Server เช่น ใช้โปรโตรคอล EAP-TLS ในการทำ Authentication ซึ่งในกรณีนี้ Client อาจต้องใช้ Smart Card หรือ Token ในการ Login เข้าสู่ระบบผ่านทาง Remote Access ด้วย

4. ตรวจสอบ Modem ที่เปิดทิ้งไว้ด้วยวิธี "War Dialing" อย่างสม่ำเสมอ หรือใช้ Vulnerability Scanner ที่สามารถตรวจสอบเครื่อง PC ในองค์กรว่ามีการเปิดใช้ Modem อย่างไม่ถูกต้องหรือไม่

5. ถ้า Remote Access User ใช้ Password เดียวกัน ในการติดต่อผ่าน Remote Access และติดต่อผ่านทาง LAN เวลาใช้งานอยู่ในองค์กร เพื่อป้องกันปัญหา DoS Attack ดังที่ได้กล่าวมาแล้ว สามารถกำหนด Policy ให้ Account Lockout เฉพาะ Remote Access เท่านั้น แต่จะไม่ Lockout ในระบบ LAN

6. ระวังการใช้งาน Remote Access Client หมายถึง ตัว Client เองควรมีการติดตั้งโปรแกรม Antivirus, Personal Firewall ตลอดจน Anti-Spyware Program เพื่อป้องกันไม่ให้ไวรัสเข้าสู่ระบบผ่านทาง Remote Access และควรมีการติดตั้งระบบ Strong Authentication หมายถึง ระบบที่มี Two-Factors Authentication เช่น Smart Card หรือ Token ตลอดจนการใช้ Digital Certificate จาก CA เพื่อเพิ่มระดับความปลอดภัยอีกชั้นหนึ่ง

จะเห็นได้ว่า Remote Access Security เป็นเรื่องที่ไม่สามารถมองข้ามได้เลย เราต้องกำหนดนโยบายการใช้งานให้รัดกุม และหมั่นตรวจสอบระบบอย่างสม่ำเสมอ ก็จะสามารถป้องกันปัญหาไม่ให้เกิดขึ้นกับระบบ Remote Access และระบบ LAN ภายในของเราได้ในที่สุด

จาก : หนังสือ eWeek Thailand

ปักษ์หลัง เดือนกรกฎาคม 2547

Update Information : 30 กรกฎาคม 2547